Claims Amended for Clarity

Claim 1 (amended) Method for the secure and controlled loading of applications onto a conventional file system smart card without the benefit of card based cryptographic services or card operating system customizations consisting of the following steps:

preloading of a plurality of small binary files that will each store the current master "card unlock key" value where each binary file can be freely updated, but read only with the proper access authorization.

access authorization to the single use binary files is selectively disclosed to third party application providers in order to grant access for application loading;

application providers retrieve the current master "card unlock key" value from the binary file to which they have been given access;

the master "card unlock key" is then used to unlock the card and ready it for application loading;

after the card is loaded with the desired application, the master "card unlock key" value is changed to a random number and its new value rewritten to all of the binary files;

the specific binary file from where the application provider first retrieved the master "card unlock key" file is then rendered unusable thereby restricting these as one time only keys.

Claim 2 (deleted)

Claim 3 (deleted)

Claim 4 (deleted)

Claim 5 (amended) Method of claim 1 wherein a master "card unlock key" value for card unlock is randomly generated after each use and is therefore different for each card and each session.

Claim 6 (amended) Method of claim 1 further consisting of a second "card unlock key" known only to a card issuer which could override any other card operations thereby allowing specific applications to be deactivated.

Claim 7 (original) Method of claim 1 wherein the said application loading can take place even after the card has been placed into circulation.

Claim 8 (original) Method of claim 1 wherein the said application loading is dynamic thereby affording greater flexibility than attempting to fit applications into a predefined card template.

Claim 9 (original) Method of claim 1 to also include the unloading of applications.

Claim 10 (amended) Method embodied as a software computer program for the Card Issuer to selectively empower third parties to be able to load applications to the smart card consisting of the following steps:

assign to the third party a previously unallocated binary file that has been preloaded on the card;

invoke the permission allocated to the third party for read access to their assigned binary file most likely in the form of presenting a key to the card;

execute the master "card unlock key" value as read from the binary file in order to unlock the card;

enable the creation of files and loading of application data to the card;

derive a new master "card unlock key" and write this back to the remaining card binary files so that this method can be repeated.

Claim 11 (original) Method of claim 10 further consisting of a secure process for individually authorizing and controlling application loading.

Claim 12 (original) Method of claim 10 wherein the authorization can be granted after the card has been placed in circulation.

Claim 13 (original) Method of claim 10 wherein the Card Issuer maintains a reversionary ownership interest in the card such that applications can be inactivated or removed.

Claim 14 (deleted)

Claim 15 (deleted)

Claim 16 (deleted)